CLAIMS

We claim:

1. A method for controlling use of configuration data comprising:

programming a configurable device using the configuration data provided by a secure device, the programmed configurable device comprising:

disabled user logic; and

a comparator;

generating a configurable device authorization code;

transmitting the configurable device authorization code to the comparator;

generating a secure device authorization code;

transmitting the secure device authorization code to the comparator;

comparing the configurable device authorization code and the secure device authorization code; and

enabling the user logic if the configurable device authorization code and the secure device authorization code are identical.

2. The method of Claim 1 wherein:

generating the configurable device authorization code comprises generating a first sequence as the configurable device authorization code in a pseudo-random number generator in the

configurable device; and

generating the secure device authorization code comprises:

generating a second sequence in a pseudo-random number generator in the secure device;

transmitting the second sequence to an encryptor in the secure device;

encrypting the second sequence to generate a third sequence;

transmitting the third sequence to a decryptor in the configurable device; and

decrypting the third sequence to generate a fourth sequence, wherein the fourth sequence is the secure device authorization code.

3. The method of Claim 2 wherein the configurable device is an SRAM PLD.

4. The method of Claim 2 wherein the secure device is an EEPROM PLD.

5. The method of Claim 2 wherein the pseudo-random number generator in the secure device is a duplicate of the pseudo-random number generator in the configurable device and both pseudo-random number generators are seeded using the same seed.

6. The method of Claim 1 wherein:

generating the configurable device authorization code comprises generating a first sequence as the configurable device authorization code in a pseudo-random number generator in the

configurable device; and

generating the secure device authorization code comprises generating a second sequence as the secure device authorization code in a pseudo-random number generator in the secure device.

7. The method of Claim 6 wherein the configurable device is an SRAM PLD.

8. The method of Claim 6 wherein the secure device is an EEPROM PLD.

9. The method of Claim 6 wherein the pseudo-random number generator in the secure device is a duplicate of the pseudo-random number generator in the configurable device and both pseudo-random number generators are seeded using the same seed.

10. The method of Claim 1 wherein:

generating the configurable device authorization code comprises generating a first sequence as the configurable device authorization code in a pseudo-random number generator in the configurable device;

generating the secure device authorization code comprises:

transmitting the first sequence to an encryptor in the secure device;

encrypting the first sequence to generate a second sequence;

transmitting the second sequence to a decryptor in the configurable device; and

decrypting the second sequence to generate a third sequence, wherein the third sequence is the secure device authorization code.

11. The method of Claim 10 wherein the configurable device is an SRAM PLD.

12. The method of Claim 10 wherein the secure device is an EEPROM PLD.

13. The method of Claim 1 wherein:

generating the secure device authorization code comprises generating a first sequence as the secure device authorization code in a pseudo-random number generator in the secure device;

generating the configurable device authorization code comprises:

transmitting the first sequence to an encryptor in the secure device;

encrypting the first sequence to generate a second sequence;

transmitting the second sequence to a decryptor in the configurable device; and

decrypting the second sequence to generate a third sequence, wherein the third sequence is the configurable device authorization code.

14. A method for controlling use of configuration data comprising:

programming a configurable device using the configuration data provided by a secure device, the programmed configurable device comprising:

disabled user logic;

a decryptor;

a configurable device sequence generator; and

a comparator;

generating a configurable device authorization code using the configurable device sequence generator;

transmitting the configurable device authorization code to the comparator;

generating a first sequence in a secure device sequence generator in the secure device;

encrypting the first sequence in an encryptor in the secure device to generate a second sequence;

transmitting the second sequence to the decryptor;

decrypting the second sequence to generate a third sequence;

transmitting the third sequence as a secure device authorization code to the comparator;

comparing the secure device authorization code and the configurable device authorization code; and

enabling the user logic if the configurable device authorization code and the secure device authorization code are identical.

15. A method for controlling use of configuration data comprising:

programming a configurable device using the configuration data provided by a secure device, the programmed configurable device comprising:

disabled user logic;

a configurable device authorization code generator; and

a comparator;

generating a configurable device authorization code in the configurable device authorization code generator;

transmitting the configurable device authorization code to the comparator;

generating a secure device authorization code in a secure device authorization code generator in the secure device;

transmitting the secure device verification code to the comparator;

comparing the configurable device authorization code and the secure device authorization code; and

enabling the user logic if the configurable device authorization code and the secure device authorization code are identical.

16. A method for controlling use of configuration data comprising:

programming a configurable device using the configuration data provided by a secure device, the programmed configurable device comprising:

disabled user logic;

a configurable device sequence generator;

a decryptor; and

a comparator;

generating a first sequence in the configurable device sequence generator;

transmitting the first sequence to the comparator as a configurable device authorization code;

transmitting the first sequence to an encryptor in the secure device;

encrypting the first sequence in the secure device encryptor to generate a second sequence;

transmitting the second sequence to the decryptor;

decrypting the second sequence to generate a third sequence;

transmitting the third sequence to the comparator as a secure device authorization code;

comparing the secure device authorization code and the configurable device authorization code; and

enabling the user logic if the configurable device authorization code and the secure device authorization code are identical.

17. A system for controlling use of configuration data, the system comprising a secure device and a configurable device, the system further comprising:

disabled user logic in the configurable device;

a comparator in the configurable device;

a secure device authorization code generator configured to generate and transmit a secure device authorization code as a first input to the comparator;

a configurable device authorization code generator configured to generate and transmit a

configurable device authorization code as a second input to the comparator; and

means connected to the comparator and the user logic for enabling the user logic if the secure device authorization code and the configurable device authorization code are identical.

18. The system of Claim 17 wherein:

the configurable device generator comprises a sequence generator in the configurable device; and

the secure device generator comprises:

a sequence generator in the secure device;

an encryptor coupled to the secure device sequence generator and configured to encrypt a first sequence generated by the secure device sequence generator to generate a second sequence; and

a decryptor in the configurable device, the decryptor coupled to the encryptor and configured to decrypt the second sequence to generate a third sequence and to transmit the third sequence as the secure device authorization code to the first input of the comparator.

19. The system of Claim 18 wherein the configurable device sequence generator and the secure device sequence generator are pseudo-random number generators and further wherein the configurable device pseudo-random number generator is a duplicate of the secure device pseudo-random number generator.

20. The system of Claim 18 wherein the configurable device is an SRAM PLD.

21. The system of Claim 18 wherein the secure device is an EEPROM PLD.

22. The system of Claim 19 wherein the pseudo-random number generators are seeded using the same seed.

23. The system of Claim 17 wherein:

the configurable device authorization code generator comprises a sequence generator in the configurable device; and

the secure device authorization code generator comprises a sequence generator in the secure device.

24. The system of Claim 23 wherein the configurable device sequence generator and the secure device sequence generator are pseudo-random number generators and further wherein the configurable device pseudo-random number generator is a duplicate of the secure device pseudo-random number generator.

25. The system of Claim 23 wherein the configurable device is an SRAM PLD.

26. The system of Claim 23 wherein the secure device is an EEPROM PLD.

27. The system of Claim 24 wherein the pseudo-random number generators are seeded using the same seed.

28. The system of Claim 17 wherein:

the configurable device authorization code generator comprises a sequence generator in the configurable device configured to generate a first sequence as the configurable device authorization code; and

the secure device authorization code generator comprises:

an encryptor in the secure device, the encryptor configured to receive and encrypt the first sequence to generate a second sequence; and

a decryptor in the configurable device, the decryptor configured to receive and decrypt the second sequence to generate a third sequence and to transmit the third sequence as the secure device authorization code to the comparator.

29. The system of Claim 28 wherein the configurable device sequence generator is a pseudo-random number generator.

30. The system of Claim 28 wherein the configurable device is an SRAM PLD.

31. The system of Claim 28 wherein the secure device is an EEPROM PLD.

32. The system of Claim 17 wherein:

the secure device authorization code generator comprises a sequence generator in the secure device configured to generate a first sequence as the secure device authorization code; and

the configurable device authorization code generator comprises:

an encryptor in the secure device, the encryptor configured to receive and encrypt the first sequence to generate a second sequence; and

a decryptor in the configurable device, the decryptor configured to receive and decrypt the second sequence to generate a third sequence and to transmit the third sequence as the configurable device authorization code to the comparator.

33. A system for controlling use of configuration data comprising:

a secure device comprising:

a secure device sequence generator configured to generate a first sequence; and

an encryptor configured to receive and encrypt the first sequence to generate a second sequence; and

a configurable device comprising:

disabled user logic;

a decryptor configured to receive and decrypt the second sequence to generate a third

sequence;

a configurable device sequence generator configured to generate a fourth sequence;

a comparator configured to receive and compare the third sequence and the fourth sequence; and

means connected to the comparator and the user logic for enabling the user logic if the third and fourth sequences are identical.

34. The system of Claim 33 wherein the sequence generators are duplicate pseudo-random number generators.

35. The system of Claim 33 wherein the configurable device is an SRAM PLD.

36. The system of Claim 33 wherein the secure device is an EEPROM PLD.

37. The system of Claim 34 wherein the pseudo-random number generators are seeded using the same seed.

38. A system for controlling use of configuration data comprising:

a secure device comprising:

a secure device sequence generator configured to generate a first sequence; and

a configurable device comprising:

disabled user logic;

a configurable device sequence generator configured to generate a second sequence;

a comparator configured to receive and compare the first sequence and the second sequence; and

means connected to the comparator and the user logic for enabling the user logic if the first and second sequences are identical.

39. The system of Claim 38 wherein the sequence generators are duplicate pseudo-random number generators.

40. The system of Claim 38 wherein the configurable device is an SRAM PLD.

41. The system of Claim 38 wherein the secure device is an EEPROM PLD.

42. The system of Claim 39 wherein the pseudo-random number generators are seeded using the same seed.

43. A system for controlling use of configuration data comprising:

a configurable device comprising:

a sequence generator configured to generate a first sequence;

a secure device comprising an encryptor configured to receive and encrypt the first sequence to generate a second sequence; and

the configurable device further comprising:

disabled user logic;

a decryptor configured to receive and decrypt the second sequence to generate a third sequence;

a comparator configured to receive and compare the first sequence and the third sequence; and

means connected to the comparator and the user logic for enabling the user logic if the first and third sequences are identical.

44. The system of Claim 43 wherein the configurable device is an SRAM PLD.

45. The system of Claim 43 wherein the secure device is an EEPROM PLD.

46. An apparatus for controlling use of configuration data, the system comprising:

a secure device comprising a secure device signal generator configured to generate a secure device signal;

a machine readable configuration data storage medium on which is provided programming

instructions for controlling use of configuration data, the instructions comprising programming instructions for:

installing disabled user logic in the configurable device;

implementing a configurable device authorization code generator in the configurable device configured to generate a configurable device authorization code;

implementing a comparator in the configurable device configured to receive and compare the configurable device authorization code and a secure device authorization code that is based on the secure device signal; and

enabling the user logic if the configurable device authorization code and the secure device authorization code are identical.

47. The apparatus of Claim 46 wherein:

the secure device signal generator comprises:

a sequence generator configured to generate a first sequence;

an encryptor configured to receive and encrypt the first sequence to generate a second sequence as the secure device signal; and

further wherein the programming instructions further comprise programming instructions for

implementing a decryptor in the configurable device, the decryptor configured to receive and decrypt the second sequence to generate a third sequence as the secure device authorization code.

48. The apparatus of Claim 46 wherein:

the secure device signal generator comprises a sequence generator configured to generate a first sequence as the secure device signal; and

the programming instructions for implementing the comparator further include the comparator receiving the secure device signal as the secure device authorization code.

49. The apparatus of Claim 46 wherein:

the secure device signal generator comprises an encryptor configured to receive and encrypt the configurable device authorization code to generate the secure device signal; and

the programming instructions further comprise programming instructions for implementing a decryptor in the configurable device, the decryptor configured to receive and decrypt the secure device signal to generate the secure device authorization code.

50. The apparatus of Claim 46 wherein:

the secure device signal generator comprises a sequence generator configured to generate a first sequence as the secure device signal;

the secure device further comprises an encryptor configured to receive and encrypt the first sequence to generate a second sequence;

the programming instructions for implementing the configurable device authorization code generator comprise implementing a decryptor in the configurable device, the decryptor configured to receive and decrypt the second sequence to generate a third sequence; and

the programming instructions for implementing the comparator further comprise implementing the comparator to receive the secure device signal as the secure device authorization code and to receive the third sequence as the configurable device authorization code.